(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－49584

(43)公開日　平成10年(1998)２月20日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ			技術表示箇所
Ｇ０６Ｆ	17/60			Ｇ０６Ｆ	15/21	Ｚ	
	1/00	３７０			1/00	３７０Ｆ	
	15/00	３３０			15/00	３３０Ｚ	
Ｈ０４Ｍ	15/00			Ｈ０４Ｍ	15/00	Ｚ	

審査請求　未請求　請求項の数14　ＯＬ　（全 15 頁）

(21)出願番号　特願平8－205952

(22)出願日　平成８年(1996)８月５日

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号

(72)発明者　岩村　恵市
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内

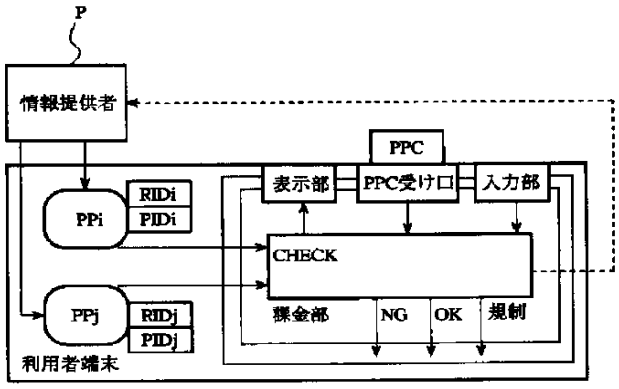
(74)代理人　弁理士　大塚　康徳　（外１名）

(54)【発明の名称】　課金システムおよびその方法

(57)【要約】

【課題】　超流通は、情報の流通を対象にするシステムであり、情報の改変には対応していないので、利用者は、その用途に応じて提供情報を改変することはできない。

【解決手段】　マルチメディアネットワークを介して、マルチメディア情報と、そのマルチメディア情報に固有の課金情報および改変情報とを受信し、受信した課金情報および金銭情報が記録された媒体の金銭情報に基づき、受信したマルチメディア情報の利用可否を判定し、受信した改変情報および金銭情報に基づき、受信したマルチメディア情報の改変の可否を判定する。



【特許請求の範囲】
【請求項１】　マルチメディアネットワークを介した情報の提供に課金するための課金システムであって、
前記マルチメディアネットワークを介して、マルチメディア情報と、そのマルチメディア情報に固有の改変情報とを受信する受信手段と、
金銭情報が記録された媒体の金銭情報を操作する操作手段と、
前記改変情報および前記金銭情報に基づき、前記受信手段により受信されたマルチメディア情報の改変の可否を判定する判定手段とを備えることを特徴とする課金システム。
【請求項２】　前記判定手段は、改変可の判定を得た場合、前記改変情報に含まれる改変および改変利用に関する許諾条件および料金を出力することを特徴とする請求項1に記載された課金システム。
【請求項３】　前記判定手段は、改変可の判定を得たマルチメディア情報の改変が指示された場合、前記許諾条件に基づく規制情報を出力することを特徴とする請求項3に記載された課金システム。
【請求項４】　前記受信手段は、さらに、前記マルチメディア情報に固有の課金情報を受信し、前記判定手段は、前記課金情報および前記金銭情報に基づき、前記受信手段により受信されたマルチメディア情報の利用可否を判定することを特徴とする請求項1に記載された課金システム。
【請求項５】　さらに、前記判定手段により得られる判定結果に基づき前記課金情報を更新する更新手段を備えることを特徴とする請求項4に記載された課金システム。
【請求項６】　前記更新手段は、前記判定手段により購入可の判定が得られた場合、前記課金情報に販売済みであることを示す情報を記録することを特徴とする請求項5に記載された課金システム。
【請求項７】　前記判定手段は、前記マルチメディア情報の利用および/または改変の可否を段階的に判定することを特徴とする請求項1から請求項4の何れかに記載された課金システム。
【請求項８】　前記操作手段は、前記判定手段による判定または指示に基づき、前記媒体の金銭情報を操作することを特徴とする請求項1から請求項7の何れかに記載された課金システム。
【請求項９】　前記金銭情報が記録された媒体はプリペイドカードであることを特徴とする請求項1から請求項8の何れかに記載された課金システム。
【請求項１０】　前記金銭情報は、前記媒体に磁気的または電子的に記録された情報であることを特徴とする請求項1から請求項8の何れかに記載された課金システム。
【請求項１１】　前記課金情報に応じた金銭情報が記録された前記媒体を用いることを特徴とする請求項1から請求項8の何れかに記載された課金システム。
【請求項１２】　前記操作手段は、前記ネットワークを介して前記金銭情報および/または前記マルチメディア情報の利用情報を入出力することを特徴とする請求項1から請求項8の何れかに記載された課金システム。
【請求項１３】　前記操作手段から前記マルチメディア情報の利用情報を受信した料金分配者は、その利用情報に見合う料金を前記マルチメディア情報の提供者に分配することを特徴とする請求項12に記載された課金システム。
【請求項１４】　マルチメディアネットワークを介した情報の提供に課金するための課金方法であって、
前記マルチメディアネットワークを介して、マルチメディア情報と、そのマルチメディア情報に固有の改変情報とを受信する受信ステップと、
金銭情報が記録された媒体の金銭情報を操作する操作ステップと、
前記改変情報および前記金銭情報に基づき、前記受信ステップで受信したマルチメディアア情報の改変の可否を判定する判定ステップとを備えることを特徴とする課金方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は課金システムおよびその方法に関し、例えば、動画像、静止画像、サウンド、コンピュータプログラム、その他データを含む情報を伝送し提供するマルチメディアネットワークにおける課金システムおよびその方法に関するものである。
【０００２】
【従来の技術】近年、幹線通信網における光ファイバネットワークの整備、ケーブルテレビシステムの普及、衛星通信の実用化、ローカルエリアネットワークの普及などが急速に進んだ。さらに、これらの通信網の相互接続も積極的になされている。これらの通信網を用いて、キャラクタデータ、静止画、サウンド、動画などを含む所謂マルチメディア情報が世界的な規模で交換されるようになった。
【０００３】これに伴い、かかる通信網を利用して様々な情報を提供し、その情報の内容および量に応じて料金を徴収する、所謂情報サービス産業が増大している。このようなサービスにおいては、提供した情報に対する課金を適切に行うことが重要である。さらに、ディジタルデータであるマルチメディア情報は、編集や変形といった情報の改変が容易であり、情報の配布や売買といった流通だけでなく、提供情報の改変についても適切に課金することができる技術が必要になる。
【０００４】また、情報の保護は不完全であり、プログラムやサウンドを含む映像情報の不正利用が問題になっている。情報の不正利用を防ぐために、コピー防止機能を付けたり、コンピュータなどに付与されているハード

ウェア機番に相当する番号をソフトウェアにも付与して、ソフトウェアの実行時に、二つの番号を照合する、などの方法がある。しかし、コピー防止機能は、ソフトウェアをバックアップする際などに不便だし、番号を照合する方法は、番号の管理や販売に関して不便であり、あまり実用的ではない。

【０００５】それに対して、「超流通」というソフトウェア権利者（以後「情報提供者」という）の権利保護を目指した概念が森亮一氏によって提案され、特開昭60-77218、特開昭60-191322、特開昭64-68835、特開平2-44447、特開平4-64129などに示されている。

【０００６】図1は特開平4-64129に示された超流通の概念図である。情報提供者Pは、提供するソフトウェアPPi（またはPPj）の利用可否を、ソフトウェアに固有のデータPIDi（またはPIDj）と、利用者のUSER-IDごとの条件によってCHECKで判定し、利用可ならばソフトウェアの利用履歴をSHに記録する。そして、情報提供者Pは、履歴に基づきソフトウェアの利用料金を請求する。なお、図に示すSSUは、以上の各手段を含むソフトウェアサービスユニットである。

【０００７】

【発明が解決しようとする課題】しかし、上述した技術においては、次のような問題点がある。

【０００８】(1)超流通は、情報提供者に情報の利用が許可された利用者であるかどうかを利用者に固有のデータによって判定する。そのため、超流通の実現手段は、少なくとも利用者に固有のデータを格納する格納手段を有する。従って、情報を利用しようとする者は、予め情報提供者に情報の利用を申し込み、USER-IDを得、利用者固有データとして登録する必要がある。利用申し込み手続や、多数の利用者固有データ(USER-ID)の管理は煩雑である。

【０００９】(2)情報の不正利用を防止するため、または、提供する情報の利用状況を情報提供者が把握するために、超流通の実現手段は、情報の利用履歴を格納する格納手段を備えている。情報提供者は、この履歴に基いて利用者に料金を請求する。超流通においては、情報は買い取りではなくレンタル的な扱いをするため、利用履歴が必要になる。しかし、利用者がどのような情報を利用したかという利用履歴は利用者のプライバシに関わり、利用者のプライバシをどのように保護するかという課題がある。

【００１０】(3)超流通は、提供情報の利用状態を正しく把握する、すなわち料金を正しく課するための手段および方式であるが、料金の支払いに関する手段や方式を含んでいない。従って、情報提供者は超流通以外の手段により料金の請求および徴収を行う必要がある。

【００１１】(4)超流通は、提供情報をレンタル的に用いることを目的に構成されているので、情報の販売には対応していない。つまり、不正利用を防止するために、ソフトウェアに固有のデータを利用者が書き換えることは禁止され、利用者が提供情報の購入を希望する場合でも、ソフトウェアに固有のデータを書き換えることはできない。

【００１２】(5)超流通は、文字どおり情報の流通を対象にするシステムであり、情報の改変には対応していないので、利用者は、その用途に応じて提供情報を改変することはできない。情報の改変には著作権などの種々の問題が付き纏うが、これらの問題を考慮した、情報の改変が可能なシステムが望まれる。

【００１３】本発明は、上述した問題を個々に、または、まとめて解決するためのものであり、利用申し込み手続や、多数の利用者固有データの管理が不要な課金システムおよびその方法を提供することを目的とする。

【００１４】また、利用者のプライバシを保護することができる課金システムおよびその方法を提供することを他の目的とする。

【００１５】また、料金の請求および徴収が容易な課金システムおよびその方法を提供することを他の目的とする。

【００１６】また、情報の販売に対応することができる課金システムおよびその方法を提供することを他の目的とする。

【００１７】著作権などの種々の問題を考慮した、情報の改変が可能な課金システムおよびその方法を提供することを他の目的とする。

【００１８】

【課題を解決するための手段】本発明は、前記の目的を達成する一手段として、以下の構成を備える。

【００１９】本発明にかかる課金システムは、マルチメディアネットワークを介した情報の提供に課金するための課金システムであって、前記マルチメディアネットワークを介して、マルチメディア情報と、そのマルチメディア情報に固有の改変情報とを受信する受信手段と、金銭情報が記録された媒体の金銭情報を操作する操作手段と、前記課金情報および前記金銭情報に基づき、前記受信手段により受信されたマルチメディア情報の利用可否を判定し、前記改変情報および前記金銭情報に基づき、前記マルチメディア情報の利用可否を判定する判定手段とを有することを特徴とする。

【００２０】また、本発明にかかる課金方法は、マルチメディアネットワークを介した情報の提供に課金するための課金方法であって、前記マルチメディアネットワークを介して、マルチメディア情報と、そのマルチメディア情報に固有の改変情報とを受信する受信ステップと、金銭情報が記録された媒体の金銭情報を操作する操作ステップと、前記改変情報および前記金銭情報に基づき、前記受信ステップで受信したマルチメディア情報の改変の可否を判定する判定ステップとを有することを特徴とする。

【００２１】
【発明の実施の形態】以下、本発明にかかる一実施形態の課金システムを図面を参照して詳細に説明する。
【００２２】
【第1実施形態】図2は本発明にかかる第1実施形態の課金方式を示す図である。図2において、Pは情報提供者、PPi（またはPPj）はPによって提供される有償の情報、PIDi（またはPIDj）はPPiに固有の情報固有データ、PPCは金銭情報、CHECKは利用可否の判定部である。
【００２３】情報提供者Pは、PIDを含めた形で情報PPを提供する。情報PPは、パーソナルコンピュータなどの利用者端末において利用される際、必ず課金部を経由するように構成してあり、その課金部には金銭情報であるPPCの受け口がある。
【００２４】情報PPの利用要求が生じると、利用可否判定部CHECKは、PIDおよびPPCの少なくとも一部の情報に基づいて、情報PPの利用の可否をチェックし、判定結果を利用者端末に通知する。例えば、CHECKは、PIDに示された利用料金がPPCの金銭情報以内であるか否かなどのチェックを行う。もし、CHECKの判定結果がOKであれば、利用者端末において情報PPの利用が可能になる。このときのPIDやPPCに関する情報、つまりPPの利用料金やPPCの残高などは、表示部に表示される。また、CHECKによる判定結果も表示部に表示することができる。
【００２５】PPCには、現金、プリペイドカードなどが利用できるが、記憶媒体（フロッピディスク、磁気カード、ICカード、PCMCIAカードなど）に格納された金銭と等価な電子的情報、所謂ディジキャッシュや電子マネーと呼ばれるものであってもよい。
【００２６】すなわち、本実施形態においては、利用者ごとの固有データUSER-IDを用いる代わりに、利用者に依存しない金銭情報PPCによって情報PPの利用可否を判定する。従って、利用者は、USER-IDなどを得るための申込手続をする必要がなく、実際の金銭、または金銭と等価な金銭情報PPCをもつだけでよい。つまり、利用者は、利用する情報PPの利用料を支払うだけである。また、多数の利用者固有データを管理する必要がなく、前述した課題(1)を解決することができる。
【００２７】また、本実施形態においては、利用者固有データを必要としないため、情報提供者Pは、どの利用者が情報PPを利用したかを知ることはできない。しかし、情報提供者Pは、情報PPの利用に応じた料金が支払われさえすれば充分であり、どの利用者が情報PPを利用したかという利用者のプライバシに関わる情報を知る必要はない。従って、前述した課題(2)を解決することができる。
【００２８】従って、本実施形態においては、どのUSER-IDをもつ利用者が、どの情報PPを利用したかという利用履歴を格納する格納部をもたないが、どの情報PPが何度利用されたかという利用頻度を格納する格納部、または、情報PPを現在利用していることを知らせる利用通知部を有することはできる。図2においては、点線で示す経路により、利用通知が情報提供者Pに送られる。具体的な利用頻度格納部または利用通知部は後述する実施形態で詳細に説明する。
【００２９】本実施形態においては、PPCは金銭と等価な情報であるので、PPCを用いること自体が料金の支払いに相当する。これにより、前述した課題(3)も解決されるが、具体的なPPCの入手法と回収法、および料金の分配法は、課題(2)と絡めて後述する実施形態に示す。
【００３０】さらに、課題(4)に関しては、PIDに、情報PPの利用料金のほかに、情報PPの販売料金を記述し、利用者が情報PPの購入を希望し（図示しない入力部を操作することで）、かつ、PPCの残高が販売料金以上である場合に、課金部のCHECKは購入を許可するとともに、情報PPのPIDに販売された情報であることを示すデータを書き込む、あるいは、情報PPのPIDに記述された利用料金を無料に書き換える。勿論、CHECKは、情報PPの不正使用を防ぐために、購入条件を満たす場合に情報PPのPIDを書き換えるが、購入条件を満たさない場合は情報PPのPIDを書き換えることはない。なお、具体的な実施形態は後述する。
【００３１】さらに、課題(5)に関しては、PIDのほかにRIDと呼ぶ改変利用に関する許諾を示す情報を情報PPに付加することにより解決することができる。ただし、RIDはPIDに含ませることもできる。そして、利用者が情報PPの改変を希望する場合に、CHECKにより改変の可否を判定することにより、情報PPの改変に対応するシステムにすることができる。なお、図2には、課金部が利用者端末に内蔵されている例を示したが、利用者端末に外付けすることもできる。なお、具体的な実施形態は後述する。
【００３２】
【第2実施形態】以下、本発明にかかる第2実施形態の課金システムを説明する。なお、第2実施形態において、第1実施形態と略同様の構成については、同一符号を付して、その詳細説明を省略する。
【００３３】図3は第2実施形態の課金方式を示す図で、PPCが現金である場合を示している。
【００３４】課金部は、情報PPのPIDに示された利用料金を表示部に表示する。利用者は、利用料金表示に従い、PPCの受け口に所定の金銭（例えばコインや紙幣）を投入する。CHECKは、投入金額がPIDに示された料金を超えたとき、情報PPの利用を許可する。
【００３５】また、時間に応じて料金が更新される場合、課金部は、その旨を表示部に表示し、利用者に追加料金を投入させるようにする。また、不図示の入力部などにより使用条件を設定する場合、課金部は、それに応じた料金を表示部に表示し、利用者に料金を投入させるようにする。つまり、CHECKは、時間や設定された使用

条件、追加投入された金額、PIDに記述された料金に基づき、再判定を行うように構成されている。

【００３６】投入された金銭は、COIN BOXに格納され、情報提供者Pまたは料金の回収を行う機関により回収される。このとき、CNTに記録された情報PPごとの利用頻度情報も回収され、その利用頻度情報に応じてCOIN BOXから回収した金額が各情報提供者Pに分配される。勿論、提供する情報PPが一つであるなど、利用頻度情報が不要の場合は、CNTを省略することができる。

【００３７】このように、本実施形態に示す現金を用いた課金方式により、情報提供者または料金分配者が、例えば、公衆電話ボックス、ゲームセンタ、喫茶店、図書館などに利用者端末を設置すれば、設置された利用者端末を、多数の人が現金を用いて利用することができる課金システムを実現することができる。

【００３８】

【第3実施形態】以下、本発明にかかる第3実施形態の課金システムを説明する。なお、第3実施形態において、第1実施形態と略同様の構成については、同一符号を付して、その詳細説明を省略する。

【００３９】図4は第3実施形態の課金方式を示す図で、PPCがプリペイドカードの場合を示している。

【００４０】利用者は、PPCの受け口にプリペイドカードを挿入する。CHECKは、挿入されたプリペイドカードの残高が、PIDに示される料金より多い場合には情報PPの利用を許可する。この場合、情報PPの利用料金が時間によって更新される場合も、プリペイドカードに充分な残高があれば継続して利用可能であるように、課金部は構成されている。

【００４１】また、不図示の入力部などにより使用条件が設定または変更された場合も、それに応じた金額をプリペイドカードから差し引くように、課金部は構成されている。このような利用の可否判定は、時間や使用条件に応じて、CHECKが、プリペイドカードの残高およびPIDの記述に基づき再判定を行うように構成すればよい。

【００４２】なお、プリペイドカードの初期金額にも限界があるので、PPCの受け口はプリペイドカードを追加挿入することができる構成にし、複数のプリペイドカードを連続的に使用することができる構成にするのが望ましい。

【００４３】テレホンカードなどと同様に、多種多様の販売店などで販売するようにすれば、プリペイドカードの入手は容易である。この場合、プリペイドカードの製造または販売会社が料金の分配者になり、情報提供者Pは、料金の分配者に対して登録を行うことにより、情報PPの利用に応じた料金の分配を受けることができる。勿論、プリペイドカードの販売店は、料金の分配者に含まれる。

【００４４】利用に応じた料金の分配に関しては、課金部が通信インタフェイス(I/F)を用いて利用情報を料金分配者に知らせる利用通知によって実現する。ただし、利用通知は、課金部がプリペイドカードから利用料金を差し引くときに限り出力されるように構成する。

【００４５】通信I/Fは、情報PPを通信により入手する場合にも利用することができる。従って、図5に示すように、料金分配者や、複数の情報提供者および利用者は、ネットワーク接続されていることになり、料金分配者は利用通知に応じて、所定の料金を所定の情報提供者に分配する。

【００４６】また、通信I/Fをもたない場合は、利用する情報PPに応じてプリペイドカードの種類を替えるという方法もある。この場合、CHICKは、利用される情報PPのPIDの記述と、プリペイドカードの種類とから利用可否を判定し、適切なプリペードカードが挿入されていれば、情報PPの利用を可能にする。

【００４７】また、情報PPの利用記録をプリペイドカードに記録する手段を課金部がもたせ、使用済みのプリペイドカードを回収することにより、利用に応じた料金の分配を行うこともできる。この場合、プリペイドカードの回収を促進するためには、例えば、プリペイドカードを交換する場合のカード代金と、交換ではない場合のカード代金とに差を付ける。つまり、交換の場合はカード残高に見合ったカード代金とし、交換ではない場合のカード代金はカード自体の代金を含むようにすればよい。ただし、それでも回収できない利用記録に対応する料金は、回収できた利用記録に応じた比率で分配するなどの処置を取る。

【００４８】このように、本実施形態に示すプリペイドカードを用いた課金方式により、情報提供者はCD-ROM、パソコン通信、インターネットなどを利用して、広範囲に情報を配布し、一方、料金分配者となる所定機関がプリペイドカードを作製し販売すれば、利用者は販売店などを通じてプリペイドカードを購入し、入手した情報を自宅その他の利用者端末で利用する課金システムが実現できる。

【００４９】

【第4実施形態】以下、本発明にかかる第4実施形態の課金システムを説明する。なお、第4実施形態において、第1実施形態と略同様の構成については、同一符号を付して、その詳細説明を省略する。

【００５０】図6は第4実施形態の課金方式を示す図で、書換が比較的容易な電気的または/および磁気的なデバイス、例えばフロッピディスク、ICカード、磁気カードをPPCに利用するものである。PPCに記録されている金銭情報は、銀行などの金融機関によって保証されたデータや、販売店を含む料金分配者によってのみ加算処理できる特殊なデータである。

【００５１】情報PPの利用者は、PPCの受け口にPPCを挿入する。課金部のCHECKは、PPCから金銭情報を読出し、その金額が情報PPのPIDに示された利用料金よりも多

く、かつ、そのPPCの発行元である料金分配者に利用料金の請求が可能である場合に、情報PPの利用を許可する。勿論、情報PPの利用料金が時間単位の場合でも、PPCに残高がある限りは、継続して情報PPを利用することができる。また、不図示の入力部などにより使用条件を設定、変更する場合、課金部は、その設定、変更に応じてPPCから所定の料金を差し引く。つまり、CHECKは、時間や設定された使用条件、追加投入された金額、PIDに記述された料金に基づき、再判定を行うように構成されている。

【００５２】この場合の金銭情報は、電子的に読み書き可能な情報であるから、課金部は、通信I/Fを介して所定の手続きを経て、料金分配者と金銭情報の入出力を行うことができる。

【００５３】前述した第1および第2実施形態と異なり、本実施形態における情報PPの利用者は金銭を料金分配者に直接支払うわけではない。利用者と契約を結んだ銀行や金融機関（以後「料金立替者」と呼ぶ）が、料金分配者に対して利用者の金銭支払いを保証するものである。従って、図7に示すように、料金分配者、料金立替者、複数の情報提供者および利用者は、ネットワーク接続されていることになる。

【００５４】さらに、前述した利用通知を、第3実施形態と同様に、通信I/Fを介して料金分配者へ送ることができ、情報PPの利用に応じた料金の分配が可能になる。この場合、利用料金を電子マネーとして、直接、料金分配者や情報提供者に送ることもできる。

【００５５】具体的には、次のような通信処理によって電子マネーの入金出金を実現することができる。ただし、課金部は、後述するような暗号処理部および認証処理部を有し、後述するTAなどで示すタイムスタンプを完全に管理する管理部を有する必要がある。これは、書換え可能なPPCを考慮して、金銭情報の不正な書き換えやPPCの複製を防止するたの処置である。つまり、金銭情報を認証可能にし、タイプスタンプの管理によって金銭情報のコピーなどの不正に対抗するものである。

【００５６】利用者をA、情報提供者をB、料金分配者をC、料金立替者をDとし、それぞれは署名可能な秘密鍵を秘密に保持し、通信相手はその署名を検査できる公開鍵を知っている（例えば、Aの秘密鍵をsA、公開鍵をpAとする）とする。ここで、AがBの提供する情報Piを利用する場合を考える。ただし、Xの鍵Yによる処理結果を{X}^Yで表し、利用者の各処理、および鍵やタイムスタンプTAの管理は、課金部内の安全性が保証された手段、または、各人の記憶や記録によるとする。

【００５７】［金銭情報入手処理］

(1)利用者Aは、例えばa円分の金銭情報の入力要求に、自分の登録情報iA（例えば口座番号やクレジット番号）を付加し、その情報に秘密鍵sAで署名したメッセージMAを料金分配者Cに送る。

MA = {A,{A, iA, a, TA}^sA}

【００５８】(2)料金分配者Cは、メッセージMAの署名を利用者Aの公開鍵pAで検査し、正しい情報であることを確認する。正しい情報であることを確認すると、メッセージMAから取出した登録情報iAを用いて、料金立替者Dにa円の請求を行う。その請求が受入れられると、基本単位e（例えば、情報PPが100円単位であれば100円）ごとに、金銭情報に料金配分者Cの署名鍵sCで署名したメッセージMCを利用者Aに送る。ただし、メッセージMCには、TAと異なるタイムスタンプTCiが付加される。

MC = Σ{TA,{C, e, TCi}^sC}^pA

【００５９】(3)利用者端末の課金部は、メッセージMCのそれぞれを鍵pAで復号し、さらに、料金分配者Ｃの公開鍵pCで署名を検査し、正しい情報であることを確認すると、{C, e, TCi}^sCをPPCに記録する。

【００６０】ただし、TAやTCiはタイムスタンプであり、同じ送信者からの同じタイムスタンプをもつメッセージは不正な情報であるといえる。また、TAやTCiは、タイムスタンプでなくても、シリアル番号や、偶然に一致することがない、または、少ない乱数でもよい。

【００６１】［利用情報通知処理］

(1)利用者Aが情報Piの利用を希望するとき、PPCの残高がPIDiに示される利用料金より大きければ、課金部は情報Piの利用を許可する。

【００６２】(2)利用者Aが情報Piの利用を終了するとき、または、利用中に、課金部は利用料金分の金額をPPCの残高から引き落とす。

【００６３】(3)このとき、利用者Aは、利用通知MBを料金分配者Cに送る。ただし、PPCから引き落とされた金額をbとする。

MB = {A, B,{B, b, TB}^sA}

【００６４】(4)料金分配者Cは、メッセージMBを検査し、正しい情報であることを確認すると、利用料b（またはその一部を除いた金額）を情報提供者Bへの分配金として支払う。

【００６５】以上では、料金分配者と利用者の間における暗号方式は公開鍵暗号とする例を説明したが、予め鍵が共有されていれば共通鍵暗号を用いてもよいことは明らかである。また、タイムスタンプの時間によって、各メッセージの有効期間を定めることもできる。以上において、メッセージ内の並び順は順不同であり、A, Bなどで示す利用者の識別子やタイムスタンプは、必ずしも必要でない場合がある。さらに、上記の金銭情報入手処理および利用情報通知処理の手順は一例であり、電子的な情報を金銭情報として、利用者固有データを用いずに課金処理を行うものはすべて本発明に含まれる。

【００６６】また、利用者端末が通信I/Fをもたない場合、利用者は、販売店など料金分配者に出向き、PPCに格納する金銭情報を入力してもらうことになる。また、課金部は、利用通知MBのような情報の利用記録をPPCに

記録し、そのPPCに金銭情報を入力する際に、利用記録が回収されることによって、情報の利用に応じた料金を分配することができる。このような電子的な金銭情報は、前述したように、料金分配者だけが処理できる特殊なデータである。従って、通信I/Fをもたない利用者は、PPCを用いるためには必ず販売店など料金分配者を介する必要があるので、利用記録は必ず回収でき、利用に応じた料金の分配が可能である。

【００６７】このように、本実施形態に示すフロッピディスクなどを用いた課金方式により、フロッピディスクドライブを備えたパーソナルコンピュータなどのような利用者端末では、PPCのための特別な受け口を必要としない。さらに、金銭情報の通信によるやり取りによってプリペードカードの販売店を省略可能にし、暗号および認証処理をソフト的に行うことにより、既存のネットワーク上で容易に実現可能な課金システムが構成できる。

【００６８】

【第5実施形態】以下、本発明にかかる第5実施形態の課金システムを説明する。なお、第5実施形態において、第1実施形態と略同様の構成については、同一符号を付して、その詳細説明を省略する。

【００６９】図8は第5実施形態の課金方式を示す図で、ICカードやPCMCIAのような電子的なカードをPPCに利用するものである。PPCに記録されている金銭情報は、銀行などの金融機関によって保証されたデータや、販売店を含む料金分配者によってのみ加算処理できる特殊なデータである。

【００７０】情報PPの利用者は、PPCの受け口にPPCを挿入し、所定の手続き（暗証番号の入力など）によってPPCを動作可能にする。課金部のCHECKは、PPCから金銭情報を読出し、その金額が情報PPのPIDに示された利用料金より多く、かつ、PPCの発行元である料金配分者に利用料金を請求が可能である場合に、情報PPの利用を許可する。勿論、情報PPの利用料金が時間単位の場合でも、PPCに残高がある限りは、継続して情報PPを利用することができる。また、不図示の入力部などにより使用条件を設定、変更する場合、課金部は、その設定、変更に応じてPPCから所定の料金を差し引く。つまり、CHECKは、時間や設定された使用条件、追加投入された金額、PIDに記述された料金に基づき、再判定を行うように構成されている。

【００７１】この場合の金銭情報は、電子的に読み書き可能な情報であるから、課金部は、通信I/Fを介して所定の手続きを経て、料金分配者と金銭情報の入出力を行うことができる。

【００７２】前述した第1および第2実施形態と異なり、本実施形態における情報PPの利用者は金銭を料金分配者に直接支払うわけではない。利用者と契約を結んだ銀行や金融機関（料金立替者）が、料金分配者に対して利用者の金銭支払いを保証するものである。従って、図7に示したように、料金分配者、料金立替者、複数の情報提供者および利用者は、ネットワーク接続されていることになる。

【００７３】さらに、前述した利用通知を、第3実施形態と同様に、通信I/Fを介して料金分配者へ送ることができ、情報PPの利用に応じた料金の分配が可能になる。この場合、利用料金を電子マネーとして、直接、料金分配者や情報提供者に送ることもできる。

【００７４】具体的には、次のような通信処理によって電子マネーの入金出金を実現することができる。ただし、通信や処理に関する安全性を考慮して、PPCに用いる電子的なカードは、セキュリティ機能としての暗証番号による所有者確認や、アクセス条件によるデータメモリへのアクセス制御や、後述するような暗号方式による暗号および認証を行う。このとき、暗号処理や認証処理に用いる秘密鍵は、アクセス制御されたメモリ領域に書込まれ、そのアクセス条件を満たす者（カード発行者や料金分配者など）しかアクセスできない。また、以下の課金動作もカード発行者または料金分配者以外は変更することができない。

【００７５】利用者をA、情報提供者をB、料金分配者をC、料金立替者をDとし、料金分配者Cは各利用者に対して暗号通信のための秘密鍵を共有し（例えば、AとCの間の秘密鍵をsA、BとCの間の秘密鍵をsBとする）、料金配分者Cは署名のための秘密鍵sCを保持し、それに対応する署名の検査鍵pCを公開しているものとする。以下、利用者Aが情報提供者Bにより提供される情報Piを利用する場合を考える。ただし、平文Xの鍵Yによる暗号文を{X}^Yで表し、利用者Aの各処理は、すべて上述したようなセキュリティ機能をもつPPC内で行われるものとする。

【００７６】［金銭情報入手処理］

(1)利用者Aは、例えばa円分の金銭情報の入力要求に、料金立替者Dに対応する自分の登録情報iA（例えば口座番号やクレジット番号）を付加し、その情報を料金分配者Cに送る。

MA = {A,{A, iA, a, TA}^sA}

【００７７】(2)料金分配者Cは、メッセージMAの暗号部分を利用者Aと共有する秘密鍵sAで復号し、登録情報iAを用いて、料金立替者Dにa円の請求を行う。その請求が受入れられると、金銭情報に料金配分者Cの署名鍵sCで署名したメッセージMCを利用者Aに送る。

MC = {TA,{C, a, TC}^sC}^sA

【００７８】(3)利用者Aは、メッセージMCを署名鍵sAで復号し、さらに、署名鍵sCに対応する公開鍵pCで署名を検査し、正しい情報であることを確認すると、PPCにa円分の金銭情報を加算する。

【００７９】ただし、TAやTCiはタイムスタンプであり、同じ送信者からの同じタイムスタンプをもつメッセージは不正な情報であるといえる。また、TAやTCiは、タイムスタンプでなくても、シリアル番号や、偶然に一

致することがない、または、少ない乱数でもよい。
【００８０】［利用情報通知処理］
(1)利用者Aが情報Piの利用を希望するとき、PPCの残高がPIDiに示される利用料金より大きければ、課金部は情報Piの利用を許可する。
【００８１】(2)利用者Aが情報Piの利用を終了するとき、または、利用中に、課金部は利用料金分の金額をPPCの残高から引き落とす。
【００８２】(3)このとき、課金部は、利用通知MBを料金分配者Cに送る。ただし、PPCから引き落とされた金額をbとする。
MB = {A,{A, B, b, TB}^sA}
【００８３】(4)料金分配者Cは、このメッセージMBを検査し、正しい条であることを確認すると、利用料b（またはその一部を除いた金額）を情報提供者Bへの分配金として支払う。
【００８４】次に、AとBの間の情報も暗号通信によってやり取りする場合、次の処理を前述した金銭情報入手処理と利用情報通知処理の間で行えばよい。ただし、料金分配者Cは情報提供者Bとも秘密鍵を共有しているとする。
【００８５】［利用情報処理］
(1)利用者Aは、情報提供者Bとの会話鍵の生成を依頼するため、次のメッセージを料金分配者Cに送る。
MA' = {A, B, TA'}
【００８６】(2)料金分配者Cは、会話鍵CKを生成し、次のメッセージを利用者Aに送る。
MC' = {{TC', A, CK}^sB, TA', B, CK}^sA
【００８７】(3)利用者Aは、メッセージMC'を秘密鍵sAで復号し、{TC', A, CK}^sBを情報提供者Bに送る。
【００８８】(4)情報提供者Bは、受信メッセージを署名鍵sBで復号し、会話鍵CKで暗号化した情報を利用者Aに送る。
【００８９】(5)利用者Aは、会話鍵CKで暗号化情報を復号する。
【００９０】以上では、処理を簡単にするために料金分配者と利用者の間における暗号方式は共通鍵暗号とする例を説明したが、前の実施形態と同様に、公開鍵暗号を用いてもよいことは明らかである。また、タイムスタンプの時間によって、各メッセージの有効期間を定めることもできる。以上において、メッセージ内の並び順は順不同であり、A, Bなどで示す利用者の識別子やタイムスタンプは、必ずしも必要でない場合がある。さらに、上記の金銭情報入手処理および利用情報通知処理の手順は一例であり、電子的な情報を金銭情報として、利用者固有データを用いずに課金処理を行うものはすべて本発明に含まれる。
【００９１】また、利用者端末が通信I/Fをもたない場合、利用者は、販売店など料金分配者に出向き、PPCに格納する金銭情報を入力してもらうことになる。また、課金部は、利用通知MBのような情報の利用記録をPPCに記録し、そのPPCに金銭情報を入力する際に、利用記録が回収されることによって、情報の利用に応じた料金を分配することができる。このような電子的な金銭情報は、前述したように、料金分配者だけが処理できる特殊なデータである。従って、通信I/Fをもたない利用者は、PPCを用いるためには必ず販売店など料金分配者を介する必要があるので、利用記録は必ず回収でき、利用に応じた料金の分配が可能である。
【００９２】このように、本実施形態に示すICカードやPCMCIAなどの電子的なカードを用いた課金方式により、第4実施形態の課金システムをより安全にした課金システムを実現することができる。
【００９３】
【第6実施形態】以下、本発明にかかる第6実施形態の課金システムを説明する。なお、第6実施形態において、第1実施形態と略同様の構成については、同一符号を付して、その詳細説明を省略する。
【００９４】図9は第6実施形態の課金方式を示す図で、第5実施形態と同様に電子的な金銭情報を用い、料金分配者の不要な課金方式である。複数の利用者および情報提供者と、料金立替者とは、図10に示すように、ネットワーク接続されている。さらに、PPCとして用いる電子カードは、セキュリティ機能として暗証番号による所有者確認や、アクセス条件によるデータメモリへのアクセス制御や、後述するような暗号方式による暗号および認証を行うことができる。このとき、暗号処理や認証処理に用いる秘密鍵は、アクセス制御されたメモリ領域に書込まれている。また、以下の課金動作もカード発行者または料金分配者以外は変更することができない。
【００９５】利用者をA、情報提供者をB、料金立替者をDとし、それぞれは署名可能な秘密鍵を保持し、通信相手は署名を検査することができる公開鍵を知っているものとする。例えば、利用者Aの秘密鍵をsA、公開鍵をpAとする。ここで、利用者Aが情報提供者Bが提供する情報Piを利用する場合を考える。ただし、Xの鍵Yによる処理結果を{X}^Yで表し、利用者Aにおける処理はすべて上述したようなセキュリティ機能をもつPPC内で行われる。
【００９６】［金銭情報入手処理］
(1)利用者Aは、例えばa円分の金銭情報の入力要求に、自分の登録情報iA（例えば口座番号やクレジット番号）を付加し、その情報を料金立替者Dに送る。
MA = {A,{A, iA, a, TA}^sA}
【００９７】(2)料金立替者Dは、メッセージMAの署名を利用者Aの公開鍵pAで検査し、登録情報iAが正しく、利用者Aに対してa円を支払可能であれば、a円に対応する金銭情報を秘密鍵sDで署名したメッセージMDを利用者Aに返す。
MD = {TA,{D, a, TD}^sD}^sA
【００９８】(3)利用者Aは、メッセージMDを公開鍵pAで

検査し、さらに、料金立替者Dの公開鍵pDで署名を検査し、正しい情報であることを確認すると、PPCにa円分の金銭情報を加算する。

【００９９】ただし、TAやTCiはタイムスタンプであり、同じ送信者からの同じタイムスタンプをもつメッセージは不正な情報であるといえる。また、TAやTCiは、タイムスタンプでなくても、シリアル番号や、偶然に一致することがない、または、少ない乱数でもよい。

【０１００】［利用情報通知処理］

(1)利用者Aが情報Piの利用を希望するとき、PPCの残高がPIDiに示される利用料金より大きければ、課金部は情報Piの利用を許可する。

【０１０１】(2)利用者Aが情報Piの利用を終了するとき、または、利用中に、課金部は利用料金分の金額をPPCの残高から引き落とす。

【０１０２】(3)このとき、利用者Aは、利用通知MBを情報提供者Bに送る。ただし、PPCから引き落とされた金額をbとする。

MB = {A, B, {B, b, TB}^sA}

【０１０３】(4)情報提供者Bは、メッセージMBを検査し、正しい情報であることを確認すると、利用者Aの署名{B, b, TB}^sAを料金立替者Dに示し、b円の料金を受取る。

【０１０４】利用者と情報提供者の間の情報も暗号通信によってやり取りする場合、直接、相手の公開鍵を用いて暗号通信を行うこともできるが、情報量が多い場合は、次のように共通鍵暗号による暗号通信を行うこともできる。この場合、各利用者と情報提供者の間には、共通鍵暗号手段が共有されているとする。ただし、(1)(2)において、AとBは逆であってもよい。

【０１０５】［情報利用情報処理］

(1)利用者Aは、情報提供者Bとの共通鍵CKの公開鍵pBで暗号化したメッセージを送る。

MA' = {A, B, CK, TA'}^pB

【０１０６】(2)情報提供者Bは、受信メッセージを秘密鍵sBで復号する。(3)情報提供者Bは、共通鍵CKにより共通鍵暗号化した情報を利用者Aに送る。(4)利用者Aは、共通鍵CKで共通鍵暗号化された情報を復号する。

【０１０７】以上では、説明を簡単にするために料金立替者、利用者、情報提供者の暗号方式は公開鍵暗号とする例を説明したが、前述したように共通鍵暗号を用いてもよいことは明らかである。また、タイムスタンプの時間によって、各メッセージの有効期間を定めることもできる。以上において、メッセージ内の並び順は順不同であり、A, Bなどで示す利用者の識別子やタイムスタンプは、必ずしも必要でない場合がある。さらに、上記の金銭情報入手処理および利用情報通知処理の手順は一例であり、電子的な情報を金銭情報として、利用者固有データを用いずに課金処理を行うものはすべて本発明に含まれる。

【０１０８】おのように、本実施形態に示す課金方式により、料金分配者が不要、すなわち利用者と情報提供者とが料金立替者を通して直接取引をする課金システムを実現することができる。また、この課金方式および課金システムは、将来実用化されると思われる、ある特殊なデータを金銭と同様に扱う電子マネーあるいはディジキャッシュに対しても適用可能であることは明らかである。

【０１０９】

【第7実施形態】以下、本発明にかかる第7実施形態の課金システムを説明する。なお、第7実施形態において、第1実施形態と略同様の構成については、同一符号を付して、その詳細説明を省略する。

【０１１０】図11は第7実施形態の課金方式を示す図である。

【０１１１】情報PPが利用されるだけではなく、購入されることもある場合、情報提供者Pは、情報PPのPIDに利用料金のほかに販売料金を記述しておく。利用者は、情報PPの購入を希望する場合、不図示の入力部により情報PPの購入を課金部へ指示するとともに、PPC受け口にPPCを挿入する。課金部のCHECKは、PPCの残高がPIDに示される販売料金以上の場合、情報PPの購入を許可するとともに、情報PPのPIDに販売済みであることを示すデータを書き込む。以降、CHECKは、PIDに販売済みを示すデータが書き込まれた情報PPは、PPCに関係なく、その利用を許可する。勿論、CHECKは、情報PPの不正使用を防ぐために、購入条件を満たす場合に情報PPのPIDを書き換えるが、購入条件を満たさない場合は情報PPのPIDを書き換えることはない。

【０１１２】また、図11では、説明を簡単にするために、通信I/Fに関する説明を省略したが、他の実施形態と同様に情報PPや金銭情報を通信によってやり取りする場合、通信I/F、暗号・認証部を付加することにより、料金分配者や料金立替者と通信することもできる。

【０１１３】

【第8実施形態】以下、本発明にかかる第8実施形態の課金システムを説明する。なお、第8実施形態において、第1実施形態と略同様の構成については、同一符号を付して、その詳細説明を省略する。

【０１１４】第8実施形態は、多くの販売店からなる販売システムに対しても有効な課金システムである。

【０１１５】情報提供者により異なる鍵で暗号化された多くの情報が格納されたCD-ROMが、販売店を通じて安価に販売され、そのCD-ROMを購入した利用者からの依頼に応じて情報提供者が指定情報の暗号鍵を知らせる際に、その情報の利用代金を請求する課金方式が知られている。しかし、この方式は、CD-ROMを販売する販売店にとって媒体の販売利益は得られても、CD-ROMに格納された情報を販売したことに対する利益は得られないという問題がある。本発明で示すPPCによる課金方式を、レンタ

ル的な情報の利用だけでなく、情報の買い取りに対しても用いることにより上記の問題を解決することができる。

【０１１６】すなわち、利用者は、販売店でのCD-ROMを購入すると同時に、プリペイドカードなどのPPCも購入する。そして、利用者が、情報提供者との通信（電話などを含む）によって暗号鍵を知るときに、プリペイドカードによる支払を指定することによって、情報提供者は、プリペイドカードを販売した販売店から情報の利用代金を回収することができる。この方法によれば、情報の利用代金も販売店を経由することになるので、販売店は情報利用に対する利益も得ることができる。

【０１１７】課金部は、PPCの残高を検査し、利用しようとする情報の料金以上の残高がある場合、その情報に対する暗号を復号し、かつ、PPCから料金を差し引くようにする。さらに、PPCは、その残高は換金できるようにし、情報提供者ごとに製作され販売店を通じてCD-ROMと同様に販売される。従って、この実施形態では料金分配者は不要である。

【０１１８】また、提供される情報のレンタル利用と共存させる場合は、PPCから料金を引き落とす際に、情報に固有のデータを第7実施形態のように書き換えればよい。

【０１１９】このように、本実施形態の課金システムは、多数の販売店や取次店による販売システムに対応することができ、さらに、提供される情報のレンタル利用とも共存することができる課金システムを構築することができる。

【０１２０】

【第9実施形態】以下、本発明にかかる第9実施形態の課金システムを説明する。なお、第9実施形態において、第1実施形態と略同様の構成については、同一符号を付して、その詳細説明を省略する。

【０１２１】以下では、提供される情報に編集、変形などの改作（改変）を施すことが可能なシステムにおける課金方法を説明する。図12は第9実施形態の課金方式を示す図である。

【０１２２】情報提供者Pにより提供される情報PPは、言語著作物、音楽著作物、美術著作物、映画著作物、写真著作物、プログラム著作物を含む原著作物である。著作権者である情報提供者Pは、情報PPの翻訳、編曲、変形、翻案、および、その二次著作物の利用などの、改作利用に関する許諾および料金情報を記述したRIDを情報PPに付加する。

【０１２３】利用者は、情報PPの改作利用を希望する場合、PPC受け口にPPCを挿入するとともに、キーボードやポインティングデバイスからなる入力部により改作利用を希望する情報PPiを選択または指定する。課金部のCHECKは、利用者が改作利用を希望する情報PPiのRDIiに記述された改作利用に関する許諾情報を調べ、改作利用が認められているのであれば、改作および改作利用に対応する許諾条件および料金を表示部に表示する。勿論、PPCの残高が表示することもできる。

【０１２４】利用者は、改作および改作利用が段階的に認められている場合、その段階を入力部により選択または指定する。CHECKは、利用者が希望する改作および改作利用に対応する料金がPPCの残高以内であれば、情報PPに対する改作および改作利用を許可するとともに、その料金をPPCから引き落とす。

【０１２５】さらに、CHECKは、改作および改作利用を許可する場合、RIDに記述されたその改作および改作利用に対応する規制情報を出力する。利用者端末は、改作および改作利用の許可を受けた場合、規制情報に従って、情報PPの改作を行い、改作した情報PPを利用する。ここで、規制情報には、情報PPおよび改作された情報PPについて、複製の可否（部分的複製や複製回数などの規制も含む）、移動の可否、削除の可否、上書きの可否、置換の可否、有効期限、利用制限、配布制限などの情報を含んでいる。

【０１２６】例えば、情報PPが人物が描かれた美術著作物で、その色や背景の改作は認められても、人物そのものの改作は認められない場合、その旨を示す許諾条件がRIDに記述されている。CHECKは、この許諾条件に基づき規制情報を出力する。つまり、この場合の規制情報は、例えば、情報PPのうち、人物像に対応する領域に関しては、利用者端末に改作を指示するコマンドを拒否させるものである。利用者端末は、この規制情報に従い、情報PPの人物像に対応する領域に関しては、例えばライトプロテクトを実行する。

【０１２７】図13は第9実施形態の第二例の課金方式を示す図である。

【０１２８】つまり、図13に示すように、情報PPにPIDおよびRIDを付加することにより、情報PPの流通についてはPIDに記述された情報を用い、情報PPの改作についてはRIDに記述された情報を用いることにより、情報PPの流通と改作とを一つの課金システムで実現するものである。なお、RIDをPIDに含ませることも可能である。

【０１２９】また、時間や設定された使用条件、改作および改作利用の条件などが変更される度に、PIDおよびRIDに記述された条件や料金に基づき、CHECKが再判定を行うように構成すれば、情報PPの段階的な利用や改作に対してきめ細かな課金を行うことができるシステムを構築することができる。

【０１３０】さらに、RIDに優先順位別に書き加えられる部分をもたせる、あるいは、情報PPに複数の優先順位に対応するRIDをもたせることができる。なお、優先順位とは、著作者、二次著作者、…のことである。この場合、CHECKは、優先順位順に規制情報を出力し、一次著作物に対する課金と同様に、二次以降の著作物に対する課金を行うことができる。

【０１３１】また、利用端末の機種に応じた形式の規制情報が必要になる場合もあるが、CHECKが利用端末に応じた形式の規制情報を出力するようにすれば、RIDの形式に依存しない課金システムになる。
【０１３２】また、図12および図13では、説明を簡単にするために、通信I/Fに関する説明を省略したが、他の実施形態と同様に情報PPや金銭情報を通信によってやり取りする場合、通信I/F、暗号・認証部を付加することにより、料金分配者や料金立替者と通信することもできる。
【０１３３】このように、本実施形態の課金システムによれば、提供される情報の著作権を考慮して、情報の改変が可能であり、その改変に応じて課金を行うことができる。
【０１３４】
【共通鍵暗号方式】共通鍵暗号方式は、送信者と受信者とが同一の暗号鍵を秘密に共有する暗号方式（秘密鍵暗号方式、対称暗号方式、慣用暗号方式とも呼ばれる）である。
【０１３５】共通鍵暗号方式は、適当な長さの文字列（ブロック）ごとに同じ鍵で暗号化するブロック暗号と、文字列またはビットごとに鍵を変えていくストリーム暗号とに分けることができる。ブロック暗号には、文字の順序を書換えて暗号化する転置式暗号や、文字を他の文字に換える換字式暗号などがある。この場合、転置や換字の対応表が暗号鍵になる。ストリーム暗号としては、多表を用いるビジネル暗号や、一回限りの使い捨ての鍵を用いるバーナム暗号などが知られている。これらは、池野、小山著「現代暗号理論」（電子情報通信学会、1986）の第2章および第4章に詳しく説明されている。
【０１３６】また、ブロック暗号のなかでもアルゴリズムが公開されているDES(Data Encryption Standard)やFEAL(Fast data Encipherment Algorithm)といった暗号が商用暗号として広く用いられている。これらは、辻井、笠原著「暗号と情報セキュリティ」（昭晃堂、1990）の第2章に詳しく説明されている。
【０１３７】ただし、DESやFEALはアルゴリズムを公開しているために暗号解読法も開発され、その解読法に対抗するために種々の変形が行われていることがある。例えば、後述する繰返し回数を増したり（C. H. Mayer and S. M. Matyas: "CRYPTOGRAPHY-A New Dimension in Computer Data Security", Wiley-Interscience, Appendix D, pp.679-712, 1982）、鍵を頻繁に変える（山本、岩村、松本、今井: "2乗型擬似乱数生成器とブロック暗号を用いた実用的暗号方式", 信学技報, ISEC93-29, pp.65-75, 1993）などの変形が提案されている。
【０１３８】
【公開鍵暗号方式】公開鍵暗号方式は、暗号鍵と復号鍵とが異なり、暗号鍵を公開、復号鍵を秘密に保持する暗号方式である。従って、暗号鍵を公開鍵、復号鍵を秘密鍵と呼ぶこともある。
【０１３９】公開鍵暗号は共通鍵暗号にない次のような特徴をもつ。
【０１４０】(1)暗号鍵と復号鍵とが異なり、暗号鍵を公開することができるため、暗号鍵を秘密に配送する必要がなく、鍵の配送が容易である。
【０１４１】(2)各利用者の暗号鍵は公開されているので、利用者は各自の復号鍵のみ秘密に記憶しておけばよく、鍵の管理が容易である。
【０１４２】(3)送られてきた通信文の送信者が偽者でないこと、および、その通信文が改竄されていないことを、受信者が確認するための認証機能を実現できる。
【０１４３】公開鍵暗号の暗号通信と認証通信、および、認証機能付き暗号通信は、以下のようなプロトコルによって実現される。以下では、送信者Aから受信者Bへ暗号通信、認証通信、認証機能付暗号通信を行う場合のプロトコルを示す。Aの秘密鍵をksA、公開鍵をkpAとし、Bの秘密鍵をksB、公開鍵をkpBとして、通信文Mに対して公開鍵kpを用いた暗号化操作をE(kp, M)とし、秘密の復号鍵ksを用いた復号操作をD(ks, M)と表す。
【０１４４】［暗号通信］AからBへ、通信文（平文）Mを秘密通信する場合は次の手順で行う。
【０１４５】ステップ1: Aは、Bの公開鍵kpBでMを暗号化し、暗号文CをBに送る。
C = E(kpB, M)
【０１４６】ステップ2: Bは、自分の秘密鍵ksBで暗号文Cを復号し、もとの平文Mを得る。
M = D(ksB, C)
【０１４７】受信者Bの公開鍵は、不特定多数に公開されているので、Aに限らずすべての人がBへ秘密の通信文を送ることができる。
【０１４８】［認証通信］AからBへ、通信文（平文）Mを認証通信する場合は次の手順で行う。
【０１４９】ステップ1: Aは、自分の秘密鍵ksAで送信文Sを生成しBに送る。
S = D(ksA, M)
【０１５０】ステップ2: Bは、Aの公開鍵kpAでSを復元変換し、元の平文Mを得る。
M = E(kpA, S)
【０１５１】もし、通信文Mが意味のある文であることが確認できれば、通信文Mが確かにAから送られてきたことが認証される。Aの公開鍵は、不特定多数に公開されているので、Bに限らずすべての人がAの署名文を認証できる。このような認証をディジタル署名ともいう。
【０１５２】［署名付暗号通信］AからBへ、通信文（平文）Mを署名付秘密通信する場合は次の手順で行う。
【０１５３】ステップ1: Aは、自分の秘密鍵ksAでMに署名し、署名文Sを作る。
S = D(ksA, M)

【０１５４】ステップ2: Aは、Bの公開鍵kpBで署名分Sを暗号化し、暗号文CをBに送る。
C = E(kpB, S)
【０１５５】ステップ3: Bは、自分の秘密鍵ksBでCを復号し、署名文Sを得る。
S = D(ksB, C)
【０１５６】ステップ4: Bは、Aの公開鍵kpAでSを復元変換し、元の平文Mを得る。
M = E(kpA, S)
【０１５７】もし、通信文Mが意味のある文であることが確認できたならば、通信文Mが確かにAから送られてきたことが認証される。なお、ステップ1と2、ステップ3と4の順序はそれぞれ逆転してもよい。
【０１５８】代表的な公開鍵暗号方式の例を以下に挙げる。
【０１５９】暗号通信と認証通信ができる方式: RSA暗号(R. L. Rivest, A. Shamir and L.Adleman: "A method of obtaining digital signatures and public key cryptosytems", Comm. of ACM, 1978)、R暗号(M. Rabin: "Digitalized signatures and public-key cryptosystems", MIT/LCS/TR-212, Technical Report MIT, 1979)、W暗号(H. C. Williams: "A modification of the RSA public-key encryptionprocedure", IEEE Trans. Inf. Theory, IT-26, 6, 1980)、MI暗号(松本、今井: "公開鍵暗号系の新しいアルゴリズム", 信学技報, IT82-84, 1982; T. Matsumoto and H.Imai: "A class of asymmetric cryptosystems based on polynomials over finite rings", IEEE International Symp. on Information Theory, 1983)
【０１６０】暗号通信のみができる方式: MH暗号(R. C. Merkle and M. E. Hellman: "Hiding information and signatures in trapdoor knapsacks", IEEE Trans. Inf. Theory, IT-24, 5, 1978)、GS暗号(A. Shamir and R. E. Zippel: "On the security of the Merkle-Hellman cryptographic scheme", IEEE Trans. Inf. Theory, IT-26, 3, 1980)、CR暗号(B. Chor and R. L. Rivest: "A knapsack type public key cryptosystem based on arithmetric infinite field", Proc. Crypto84)、M暗号(R. J. McEiece: "A public-key cryptosystem based on algebraiccoding theory", DSN Progress Rep., Jet Propulsion Lab., 1978)、E暗号(T.E. ElGamal: "A public key cryptosystem and a signature scheme based on discretre logarithm", Proc. Crypto 84, 1984)、T暗号(辻井重男: "行列分解を利用した公開鍵暗号の一方式", 信学技報, IT85-12, 1985)
【０１６１】認証通信のみができる方式: S暗号(A. Shamir: "A fast signature scheme",Report MIT/LCS/TM-107, MIT laboratory for computer science, Cambridge, Mass., 1978)、L暗号(K. Lieberherr: "Uniform complexity and digital signature", Lecture Notes in Computer Science 115 Automata, Language and Programming, Eighth Colloquium Acre, Israel, 1981)、GYM暗号(S. Goldwasser, S.Micali and A.Yao: "Strong signature schemes", ACM Symp. on Theory of Computing, 1983)、GMR暗号(S. Goldwasser, S. Micali and R. L. Rivest: "A 'paradoxical' solution to the signature problem", ACM Symp. on Foundationof Computer Science, 1984)、OSS暗号(H. Ong, C. P. Schnorr and A. Shamir:"An efficient signature scheme based on quadratic equation", ACM Symp.on Theory of Computing, 1984)、OS暗号(岡本、白石: "多項式演算によるディジタル署名方式", 信学論(D), J68-D, 5, 1985; T. Okamoto and A. Shiraisi:"A fast signature scheme based on quadratic in equalities", IEEE Symp. on Theory of Computing, 1984)
【０１６２】
【他の実施形態】本発明の目的は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはCPUやMPU）が記憶媒体に格納されたプログラムコードを読出し実行することによっても、達成されることは言うまでもない。この場合、記憶媒体から読出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。プログラムコードを供給するための記憶媒体としては、例えば、フロッピディスク，ハードディスク，光ディスク，光磁気ディスク，CD-ROM，CD-R，磁気テープ，不揮発性のメモリカード，ROMなどを用いることができる。
【０１６３】また、コンピュータが読出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているOS（オペレーティングシステム）などが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。
【０１６４】さらに、記憶媒体から読出されたプログラムコードが、コンピュータに挿入された機能拡張カードやコンピュータに接続された機能拡張ユニットに備わるメモリに書込まれた後、そのプログラムコードの指示に基づき、その機能拡張カードや機能拡張ユニットに備わるCPUなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。
【０１６５】このように、本発明にかかる各実施形態によれば、前述した課題(1)から(5)を解決する課金方式および課金システムを実現することができる。
【０１６６】すなわち、利用者は種々の情報をレンタル的に安価に利用し、利用者のプライバシも保護され、情

報提供者は利用者ごとの情報利用の管理を行うことなく、情報の利用に応じて利用料金の分配を受けることができる。

【０１６７】また、販売店を含む料金分配者や料金立替者を導入することにより、料金の支払いまでを含めて使い勝手のよい課金システムを構成することができる。

【０１６８】また、情報に固有でない付属データにより、情報提供者以外の、ネットワークに関する種々の提供者にも正当な料金を分配することができる柔軟な課金システムを構築することができる。

【０１６９】また、提供情報のレンタル的な利用と販売とを両立できる課金システムを構築することができる。

【０１７０】また、情報の流通だけでなく、情報の改変にも対応する課金システムを構築することができる。

【０１７１】

【発明の効果】以上説明したように、本発明によれば、利用申し込み手続や、多数の利用者固有データの管理が不要な課金システムおよびその方法を提供することができる。

【０１７２】また、利用者のプライバシを保護する課金システムおよびその方法を提供することができる。

【０１７３】また、料金の請求および徴収が容易な課金システムおよびその方法を提供することができる。

【０１７４】また、情報の販売に対応することができる課金システムおよびその方法を提供することができる。

【０１７５】著作権などの種々の問題を考慮した、情報の改変が可能な課金システムおよびその方法を提供することができる。

【図面の簡単な説明】

【図１】超流通の概念図、

【図２】第1実施形態の課金方式を示す図、

【図３】第2実施形態の課金方式を示す図、

【図４】第3実施形態の課金方式を示す図、

【図５】第3実施形態におけるネットワークを示す図、

【図６】第4実施形態の課金方式を示す図、

【図７】第4実施形態におけるネットワークを示す図、

【図８】第5実施形態の課金方式を示す図、

【図９】第6実施形態の課金方式を示す図、

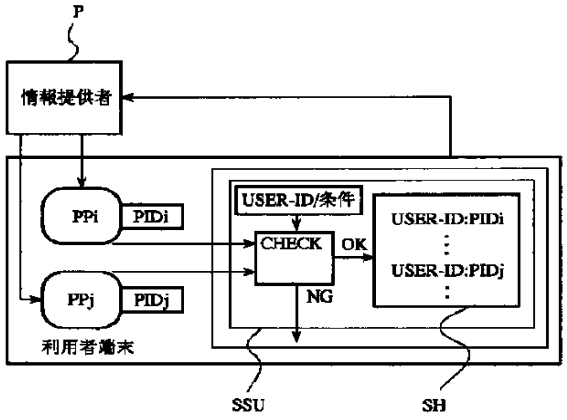
【図１０】第6実施形態におけるネットワークを示す図、

【図１１】第7実施形態の課金方式を示す図である。

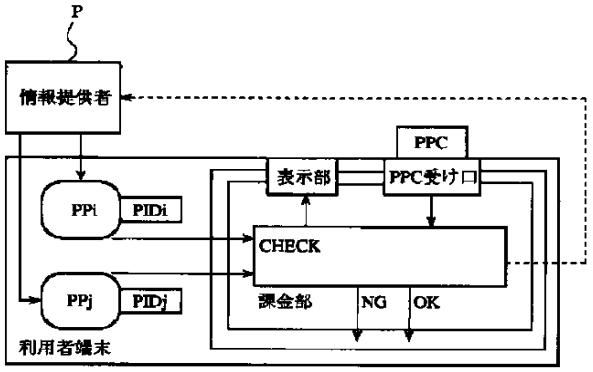
【図１２】第9実施形態の課金方式を示す図、

【図１３】第9実施形態の第二例の課金方式を示す図である。

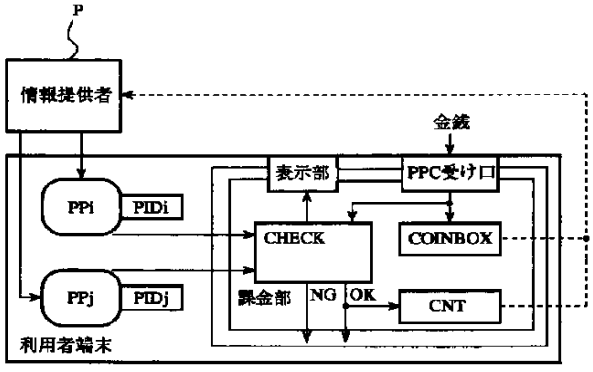
【図１】



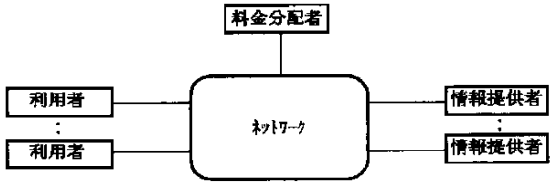
【図２】



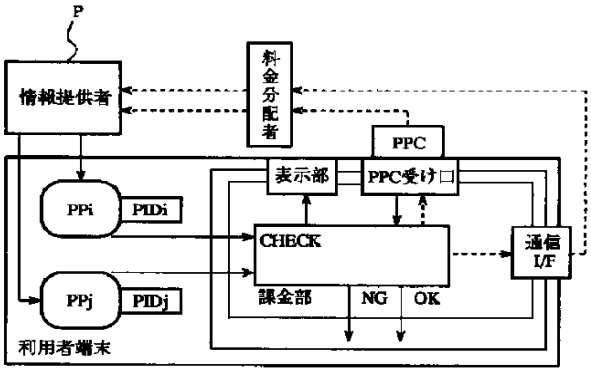
【図３】



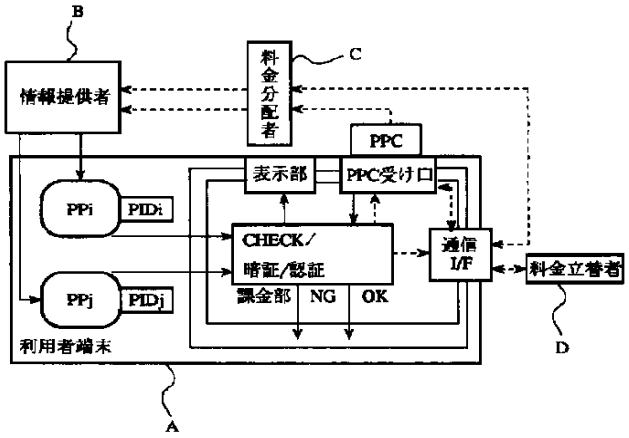
【図５】



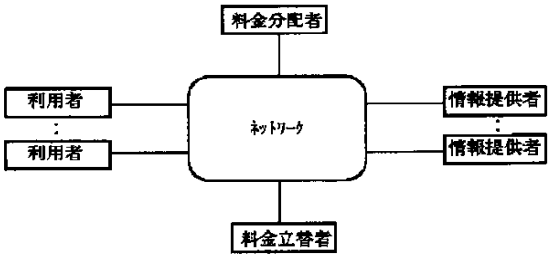
【図４】



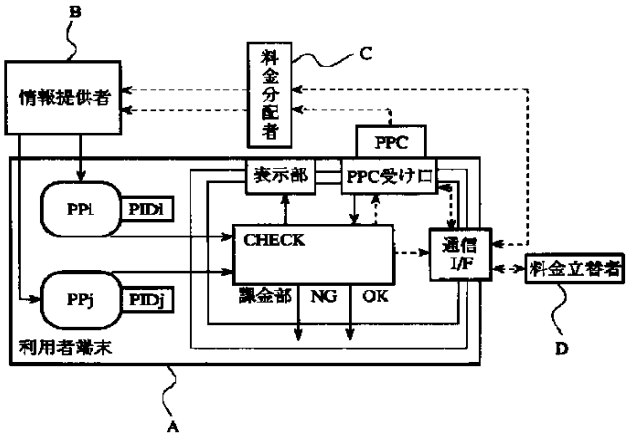
【図６】



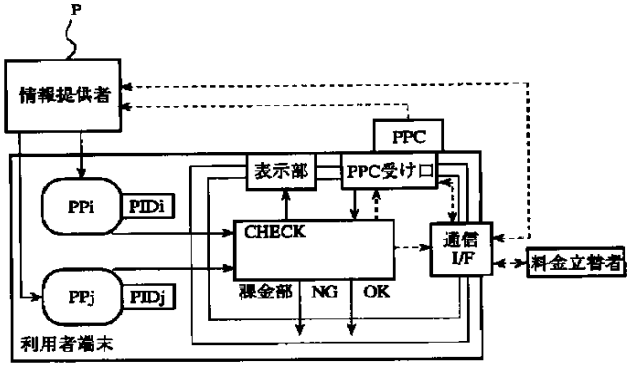
【図７】



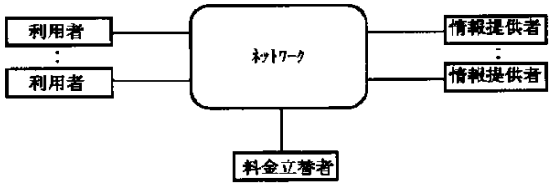
【図８】



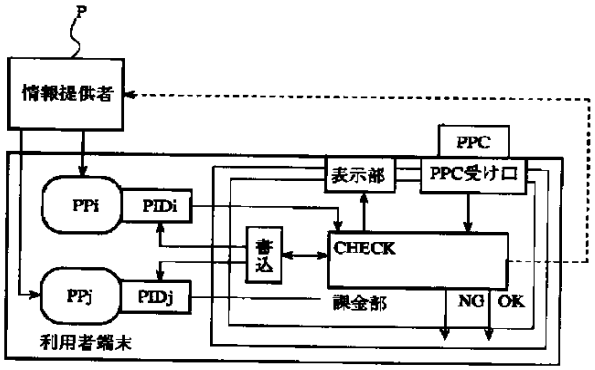
【図９】



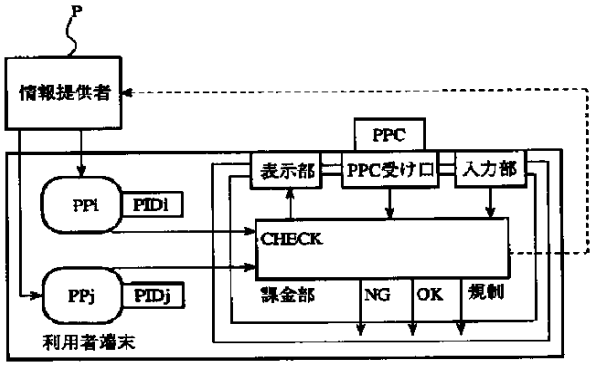
【図１０】



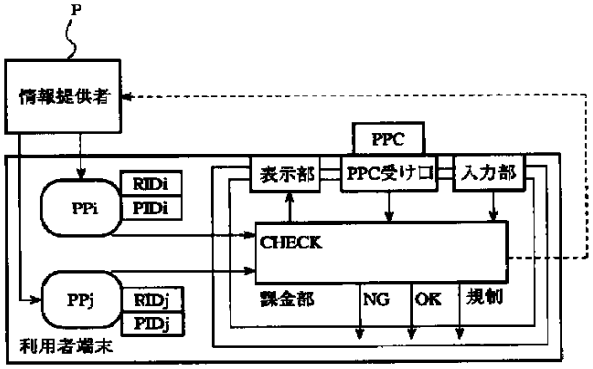
【図１１】


P
情報提供者
PPC
表示部
PPC受け口
PPi
PIDi
書込
CHECK
PPj
PIDj
課金部
NG
OK
利用者端末

【図１２】


P
情報提供者
PPC
表示部
PPC受け口
入力部
PPi
PIDi
CHECK
PPj
PIDj
課金部
NG
OK
規制
利用者端末

【図１３】


P
情報提供者
PPC
表示部
PPC受け口
入力部
PPi
RIDi
PIDi
CHECK
PPj
RIDj
PIDj
課金部
NG
OK
規制
利用者端末